25
Cybersecurity

Aan de orde is het **VAO Cybersecurity (AO d.d. 20/01)**.

De **voorzitter**:
Ik heet de leden van harte welkom, evenals de staatssecretaris. Ik geef als eerste graag het woord aan de heer Van Meenen namens de fractie van D66.

De heer **Van Meenen** (D66):
Voorzitter. De heer Verhoeven zou hier normaal gesproken staan, maar hij is helaas verhinderd. Nu valt mij deze buitengewone eer te beurt.

Ik mag de volgende motie indienen.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de afgelopen decennia tientallen databestanden van verschillende ministeries en andere organisaties gekoppeld zijn zonder toetsing op het gebied van cybersecurity;

overwegende dat dit grote aantal gekoppelde databestanden een cybersecurityrisico kan zijn en daarmee de privacy van mensen in gevaar kan brengen;

verzoekt de regering, alle gekoppelde databestanden kritisch tegen het licht te houden op het gebied van cybersecurity, en indien nodig het aantal gekoppelde databestanden terug te brengen,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Van Meenen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 386 (26643).

Ook mevrouw Gesthuizen wordt vandaag vervangen, en wel door de heer Van Nispen. Hij zal nu de inbreng namens de SP doen.

De heer **Van Nispen** (SP):
Voorzitter. U zei het al: ik dien deze motie in namens mijn collega Gesthuizen.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat de voormalig minister van Veiligheid en Justitie heeft gesteld dat het mogelijk is om onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op afstand een computersysteem te betreden;

constaterende dat bij de invoering van de bevoegdheid om een plaats te doorzoeken echter nooit is gesproken over het op afstand binnendringen van computers en dat, indien voor een dergelijk handelen een wettelijke grondslag zal worden gecreëerd, dit in de eerste plaats iets is waarover de Kamer zich zal moeten uitspreken;

verzoekt de regering, te garanderen dat politie en justitie in ieder geval niet overgaan tot het op afstand heimelijk binnendringen van een geautomatiseerd werk zolang de wet computercriminaliteit III niet door de Kamer is behandeld en zij zich hierover heeft kunnen uitspreken,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door de leden Van Nispen en Gesthuizen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 387 (26643).

Mevrouw **Tellegen** (VVD):
Voorzitter. Vorige week vrijdag stond er nog een groot artikel in Het Financieele Dagblad met als titel De ondraaglijke complexiteit van software. Ook in dit artikel wordt weer heel duidelijk dat storingen door softwarefouten steeds vaker voorkomen. Daarmee neemt het risico op beveiligingslekken in digitale systemen, ook binnen onze vitale infrastructuur, toe. Legacy, het Engelse woord voor verouderde ICT-systemen, moet dan ook bijtijds worden vervangen om die risico's te minimaliseren. Ik heb hier tijdens het AO aandacht voor gevraagd. Ik wil de staatssecretaris met de volgende motie aansporen op het gebied van het vervangen van oude ICT-systemen.

Motie

De Kamer,

gehoord de beraadslaging,

constaterende dat het Cybersecuritybeeld Nederland 5 aangeeft dat de beschikbaarheid van digitale systemen steeds belangrijker wordt omdat belangrijke maatschappelijke processen hiervan afhankelijk zijn en analoge alternatieven steeds vaker ontbreken;

constaterende dat legacy bestaat uit ICT-systemen met verouderde software en hardware met een verhoogd risico op beveiligingslekken, waardoor het risico op hacks en storingen toeneemt en digitale systemen kwetsbaar worden;

overwegende dat binnen de Nederlandse vitale infrastructuur en diensten digitale systemen met legacy worden gebruikt en dit onnodig risico oplevert voor belangrijke maatschappelijke processen en daarmee voor de nationale

veiligheid, mede door koppeling van verschillende vitale infrastructuren en ketenafhankelijkheden;

van mening dat legacy in de Nederlandse vitale infrastructuur, bij zowel de overheid als vitale sectoren, zo spoedig mogelijk moet worden vervangen en dat de rijksoverheid hierin een voorbeeldfunctie heeft;

verzoekt de regering, de legacyproblematiek actief, zowel binnen de rijksoverheid als binnen de vitale sectoren, tegen te gaan en daarbij dit punt in de toegezegde doorontwikkeling van de nationale cybersecuritystrategie te betrekken;

verzoekt de regering tevens om dit punt actief op te pakken in het kader van de implementatie van de NIB-richtlijn in het kader van sectorale zorgplichten op het gebied van digitale veiligheid,

en gaat over tot de orde van de dag.

De **voorzitter**:
Deze motie is voorgesteld door het lid Tellegen. Naar mij blijkt, wordt de indiening ervan voldoende ondersteund.

Zij krijgt nr. 388 (26643).

Hiermee zijn wij gekomen aan het eind van de inbreng van de Kamer. Wij wachten even tot ook de laatste motie is rondgedeeld.

De vergadering wordt enkele ogenblikken geschorst.

☐

Staatssecretaris **Dijkhoff**:
Voorzitter. Ik ga eerst in op de motie van de heer Van Meenen, op stuk nr. 386. Die gaat over de gekoppelde databestanden. We hebben natuurlijk een inventarisatie van die bestanden gemaakt. Nou snap ik dat er een vervolgvraag is op dit punt, maar ik vind het een beetje een aparte focus. We checken alle systemen waarvoor we verantwoordelijk zijn. Daarvoor zijn we sowieso verantwoordelijk, gezien vanuit het cybersecuritybeleid. We moeten daarbij vooral ook naar de kwetsbaarheden kijken. Ik vind het geen goed idee om nu een aparte "zijtak" te maken waarbij koppelingen worden bekeken. Het bekijken van de koppelingen vormt gewoon een integraal onderdeel van het bezien van de integrale veiligheid van de systemen. Ze worden bekeken op kwetsbaarheden. Wat mevrouw Tellegen in haar motie aangeeft, is daar ook een aspect van; daarop zal ik zo terugkomen. Al die aspecten nemen we in het reguliere beleid mee. Daarbij horen dus ook de gekoppelde bestanden. Ik vind het geen goed idee om de koppeling zelf weer op cybersecurity te gaan controleren. Dat is namelijk al onderdeel van bestaand beleid. Ik zie niet wat een soort speciale doorlichting gericht op die gekoppelde databestanden zou toevoegen aan de cybersecurity en aan ons beleid in brede zin. Daarom ontraad ik deze motie.

Ik heb de indruk dat er bij de motie op stuk nr. 387, die is ingediend door de heer Van Nispen, sprake is van wat misverstand. Je kunt dit op twee manieren opvatten. Er is enerzijds sprake van artikel 125i van het Wetboek van Strafvordering, en van wat er in het verleden al is gebeurd. Er wordt nu om een moratorium gevraagd. Anderzijds is er echter wat het wetsvoorstel Computercriminaliteit III geeft. Dat gaat over iets anders. In het wetsvoorstel komt een bevoegdheid, onder strikte voorwaarden, te staan om van een afstand — plat gezegd: vanuit het politiebureau — in een systeem te komen. We zullen het daar nog uitgebreid over hebben. Onder artikel 125i is het volgende al toegestaan. Er is een computer van iemand, je bent daar fysiek bij en je gaat die computer onderzoeken. Dat doe je natuurlijk niet zomaar; daarvoor heb je toestemming gekregen. Daarbij kunnen zaken worden aangetroffen, bijvoorbeeld — ik maak het even heel beeldend — een link naar iets in de cloud. Technisch gezien ben je dan vanaf die computer al op afstand in een andere computer bezig. Die bevoegdheid is dus echter heel beperkt. Die begint met het fysiek aanwezig zijn van een systeem van een verdachte. Dat is dus iets wezenlijk anders dan de wettelijke grondslag waar het wetsvoorstel Computercriminaliteit III in voorziet. We hebben hier dus niet te maken met een situatie die zich al een keer heeft voorgedaan en waarvoor een grondslag eigenlijk ontbreekt, maar met twee verschillende feitelijke situaties. Voor het een bestaat gewoon een wettelijke grondslag. Het wetsvoorstel ziet op iets nieuws en op iets anders, dus buiten de huidige praktijk.

De heer **Van Nispen** (SP):
Als er sprake is van een misverstand, zou dat alleen maar goed zijn. Toch wordt ook door deskundigen betwijfeld of die wettelijke grondslag er wel is. Ik wil ook wijzen op een antwoord van toenmalig minister Opstelten op Kamervragen. Daarin schrijft hij met nadruk het volgende. "Voorts is het onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen." Dat lijkt toch wel erg veel op wat de staatssecretaris zojuist zei. Dit is dus al gebeurd. En er wordt dus door deskundigen gezegd dat de wettelijke basis ervoor ontbreekt.

Staatssecretaris **Dijkhoff**:
Nog los van hoe dit eerder is geformuleerd, zeg ik dat er in de casus waarin dit gebeurde, sprake was van een systeem van de verdachte waarop een link werd aangetroffen. Via die link kon toegang worden verkregen tot versleutelde bestanden van die persoon. Het ging daarbij om nogal gruwelijke bestanden. Die bestanden waren op die manier via die computer van de verdachte te bezoeken. Zo is dat toen gegaan. Daar is toestemming voor verleend. Er is geen wettelijke grondslag om dat nu op een andere manier te doen, dus de manier die ik net omschreef en waar het wetsvoorstel in voorziet. Dat is nu dus ook niet staande praktijk. Zo is het in dat geval ook niet gegaan, naar mijn beste weten. Het is in ieder geval goed om dat misverstand op te helderen. De heer Van Nispen heeft het over wat deskundigen zeggen. We komen niet voor niets met dat wetsvoorstel Computercriminaliteit III, want dat is inderdaad nu niet mogelijk. Artikel 125i van het Wetboek van Strafvordering laat toe wat ik zojuist omschreef. Daarbij gaat het dus op een andere manier. Ik zie niet dat er daartussenin nog een bestaande praktijk is die nog van een wettelijke basis moet worden voorzien.

De heer **Van Nispen** (SP):
Het is ingewikkeld. Toch begrijp ik dan niet helemaal wat toenmalig minister Opstelten toen aan de Kamer heeft geschreven. Vervolgens zijn er deskundigen die zeggen dat de wettelijke grondslag ontbreekt. Ik zie dat ook zo. De vraag is dus of het klopt wat de minister toen aan de Kamer schreef. Of zegt de staatssecretaris: nou ja, toen zijn de woorden eigenlijk niet helemaal goed gekozen? Zegt hij: als het toen anders geformuleerd was, was het wellicht duidelijker geweest? Het is erg ingewikkeld, maar het is toch wel van belang om hierover voor de stemmingen misschien die duidelijkheid te krijgen.

Staatssecretaris **Dijkhoff**:
Zeker. In de omschrijving die net geciteerd wordt staat: onder voorwaarden. Dat is een beetje open. Ik heb dat toen niet uitgesproken of geschreven, maar als toen met "onder voorwaarden" werd bedoeld dat het gaat op de manier die ik net omschreef, dan is dat zo. Of misschien is het er niet mee bedoeld. Het is een beetje tekstexegese achteraf. Zoals ik het net gezegd heb, is het nu: je mag daar nu niet van afstand in. Daarom komen we ook met een nieuw wetsvoorstel. Als je een systeem aantreft en je daarop verder kunt, al was het maar met een simpele cloudlink, dan kom je technisch gezien via die computer op afstand ergens anders in, maar dan heb je wel al fysiek toegang tot een systeem van een persoon en heb je dat niet ongemerkt gedaan. In de wetsgeschiedenis moeten we straks natuurlijk opnemen hoe we dat met het nieuwe wetsvoorstel regelen. Dat is een significant andere manier van praktisch handelen. Dat onderscheid is voor mij duidelijk, het is ook duidelijk in de wet en in de huidige praktijk.

De **voorzitter**:
Daarmee ontraadt u de motie?

Staatssecretaris **Dijkhoff**:
Ja.

Dan kom ik bij de derde motie. Ik heb net even gedacht over een Nederlands voor legacyproblematiek en "ouwe meuk" komt misschien nog het dichtst in de buurt. Het is een veiligheidsrisico. In verouderde software zitten veel kwetsbaarheden, ook al patch je ze een voor een. Nieuwe software is er niet voor niets. Dat is niet alleen voor nieuwe shiny features, maar ook zodat de beveiliging beter op orde is. Het is dus zeker een verantwoordelijkheid van iedereen om dit een inherent onderdeel te laten zijn van het beleid, met name, waar mevrouw Tellegen al aan refereerde, richting de richtlijn inzake de verantwoordelijkheid voor systemen in de vitale sector. Dat is nu impliciet. Ik vind het verstandig om dat ook expliciet te maken. De technologische ontwikkelingen gaan heel erg snel. Ik zie de motie dan ook als ondersteuning van beleid. Mocht deze een Kamermeerderheid halen, dan zullen we in de reactie op het volgende Cybersecuritybeeld Nederland de aanpak expliciet naar voren brengen.

Mevrouw **Oosenbrug** (PvdA):
Ik heb een aanvullende vraag. Wordt open source daar ook in meegenomen? Daar hebben we al een paar moties over ingediend. Als we dan toch software aan het vervangen zijn, wil ik graag dat eerst wordt gekeken naar opensource-oplossingen.

Staatssecretaris **Dijkhoff**:
Ik vind daar ook van alles van, maar ik moet me dan even beperken tot mijn verantwoordelijkheid voor cybersecurity. Ik kan niet bij voorbaat stellen dat open source vanuit de veiligheid altijd een beter alternatief is. Er zijn misschien heel veel andere redenen voor. Ik kan die voorkeurspositie niet vanuit cybersecurity meenemen, maar daar heb ik menig discussie over met collega's die daar systeemverantwoordelijkheid voor dragen. Ik kan, helaas, niet als cybersecurityadvies meegeven dat het altijd beter is.

De beraadslaging wordt gesloten.

De **voorzitter**:
We hoeven over deze suggestie dinsdag niet te stemmen, zoals over de overige moties. Het zal zeker worden meegenomen in de toekomstige debatten.

De beraadslaging wordt gesloten.

De **voorzitter**:
We zijn aan het einde gekomen van dit VAO Cybersecurity. Over de moties zal aanstaande dinsdag gestemd worden. Over enkele ogenblikken gaan wij verder met het VAO Noodhulp.

De vergadering wordt enkele ogenblikken geschorst.